(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 063 862 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
27.12.2000 Patentblatt 2000/52

(51) Int. Cl.[7]: **H04Q 7/38**, H04Q 7/32

(21) Anmeldenummer: **00112588.9**

(22) Anmeldetag: **14.06.2000**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **25.06.1999 DE 19929251**

(71) Anmelder:
Fujitsu Siemens Computers GmbH
81739 München (DE)

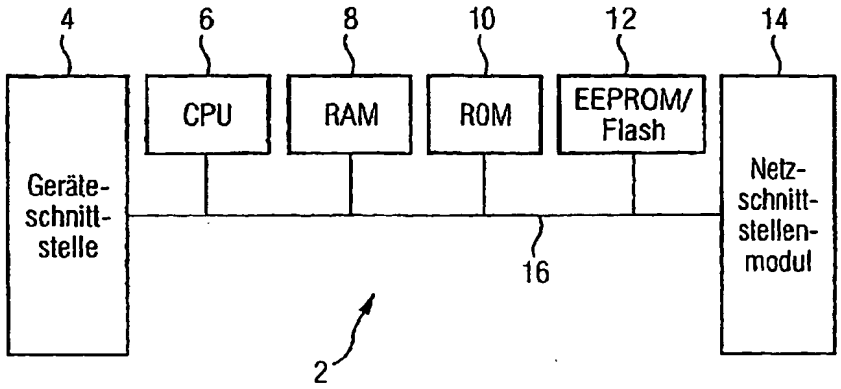
(72) Erfinder: **Wiehler, Gerhard**
82223 Eichenau (DE)

(74) Vertreter:
Epping, Wilhelm, Dipl.-Ing. et al
Epping Hermann & Fischer
Postfach 12 10 26
80034 München (DE)

(54) Verfahren und Einrichtung zum Aufbau einer Kommunikation zwischen einem Anwendergerät und einem Netz

(57) Es wird ein Verfahren und eine Einrichtung zum Aufbauen einer Kommunikation zwischen einem Anwendergerät und einem Netz angegeben, wobei persönliche Daten und Informationen sowie Programme über den Kommunikationsaufbau zwischen dem Anwendergerät und dem Netz in einem persönlichen Kommunikationsmodul gespeichert und die Daten und die Informationen zum Aufbau der Kommunikation abgerufen werden.

FIG 1



chreibung

1] Die Erfindung betrifft ein Verfahren und eine ichtung zum Aufbau einer Kommunikation zwischen m Anwendergerät und einem Netz.

2] Die mobile Kommunikation mit Mobilfunkte- ıen hat in den vergangenen Jahren einen großen chwung erlebt. Auch für andere Geräte beispiels- e Notebooks, in der Hand haltbare PC's, und vor n für eine Generation neuer Geräte, beispielsweise ınizer, Autonavigatoren, digitale Kameras, Walk- und dergleichen, wird eine flexible Anschlußmög- eit an ein Mobilnetz oder Festnetz immer wichtiger. ei wird in den nächsten Jahren die Anzahl der ver- edenen Geräte, die ein einzelner Benutzer für den ang zum Netz verwendet, ständig steigen. Auch ıten Benutzer, deren Aufenthaltsort häufig wech- mit fremden Anwendergeräten, beispielsweise den PC's, auf eigene Netzresourcen zugreifen kön- Heutige Identifizierungs- und Authentisierungsver- :n sind hier umständlich und bieten keine eichende Sicherheit.

3] Nach dem heutigen Stand der Technik hat s Anwendergerät einen eigenen Kommunikations- ıl, beispielsweise GSM, um die Kommunikation chen dem Anwendergerät und einem Netz herzu- :n. Die persönliche Identifikation beziehungsweise ntifikation des Anwenders im Netz wird in der ıf gerätespezifisch nach dem jeweiligen Verfahren Netzbetreibers, Dienstanbieters oder der Anwen- durchgeführt. Ein Benutzer, der beispielsweise ein lfunktelefon, ein Note-book, einen PC, einen Orga- , eine digitale Kamera oder einen Autonavigator mit jeweiligen Netzanschluß verwenden möchte, e demnach Geräte mit fest eingebauten, gerätе- fischen Kommunikationsmodulen benutzen müs- Dabei müssen dann gänzlich unterschiedliche ifikations- beziehungsweise Authentifikationsver- n mit den zugehörigen Paßwörtern, PIN oder ren Eingaben beherrscht werden, was sehr ıktisch ist, weil die einzelnen Identifikations- oder ntifikationsverfahren unterschiedlich sind und : das Gedächtnis des Anwenders strapazieren. der Kompliziertheit der verschiedenen Verfahren dennoch die verwendeten Identifikations- und ntisierungsverfahren für offene Netzarchitekturen sicher genug.

4] Demgegenüber liegt der Erfindung die Auf- zugrunde, ein Verfahren und eine Einrichtung zum ıu einer Kommunikation zwischen einem Anwen- rät und einem Netz bereitzustellen, welches ein- bedienbar und auf die persönlichen Bedürfnisse)aten des Anwenders abgestimmt ist.

5] Dazu ist das erfindungsgemäße Verfahren ch gekennzeichnet, daß die persönlichen Daten die Information über den Kommunikationsaufbau hen unterschiedlichen Anwendergeräten und Net- ı einem in unterschiedliche Geräten steckbaren, persönlichen Kommunikationsmodul gespeichert werden, und daß die Daten und Informationen zum Aufbau der Kommunikation abgerufen werden.

[0006] Bei dem erfindungsgemäßen Verfahren zur Identifikation oder Authentisierung in Netzen sind die persönlichen Identifikations- und Authentisierungs-Daten beziehungsweise Merkmale in dem Kommunikationsmodul in einer Moduleinheit fest miteinander verbunden. Den persönlichen Kommunikationsmodul kann der Anwender wie einen Personalausweis ständig mit sich tragen. Über eine standardisierte Schnittstelle kann der Kommunikationsmodul mit einem einfachen Handgriff gesteckt und in verschiedenen eigenen Anwendergeräten, beispielsweise Mobiltelefon, Organizer, Notebook, PC, Walkman, Kamera, Set-Top-Box und dergleichen jeweils dann eingesetzt werden, wenn ein Netzzugang gewünscht wird. Auch in fremden Geräten, die eine Standardschnittstelle zur Verfügung stellen und den Kommunikationsmodul mit entsprechender Treiber-Software bedienen können, kann der persönliche Kommunikationsmodul Verwendung finden.

[0007] Ein weiterer Vorteil besteht darin, daß die Identifikations-, Authentisierungs- und Autorisierungsprozeduren erheblich vereinfacht werden können, da beispielsweise Paßwörter, private Schlüssel, Zertifikate des öffentlichen Schlüssels, Telefonnummern und dergleichen in dem Kommunikationsmodul gespeichert sind und vom Anwender nicht mehr bei jeder Gelegenheit neu eingegeben werden müssen.

[0008] Eine vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß der persönliche Kommunikationsmodul mit den Identifikations- und Authentisierungsdaten sowie persönlichen Daten seines Besitzers beziehungsweise Anwenders mechanisch gekapselt werden. Ein Vorteil dieser Ausführungsform besteht darin, daß die Daten von außen durch Unberechtigte nicht manipuliert werden können. Da beispielsweise Paßwörter und private Schlüssel in dem verkapselten Kommunikationsmodul wesentlich sicherer gespeichert sind als nach dem Stand der Technik, ist auch eine ausreichende Sicherheit für sensitive Anwendungen im offenen Netz gegeben.

[0009] Eine vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß auch die Programme zum Kommunikationsaufbau in dem Kommunikationsmodul gespeichert werden. Damit wird der Kommunikationsmodul in vorteilhafter Weise zu einem eigenständigen Gerät, mit dem die Kommunikation hergestellt werden kann.

[0010] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß die persönlichen Daten solche zum Identifizieren oder Authentisieren sowie personenbezogene Daten umfassen. Damit wird in vorteilhafter Weise der Anwendungsbereich des Kommunikationsmoduls vergrößert, indem nicht nur die Zugangsdaten zum Aufbau der Verbindung sowie die Daten zur Identifizierung und Authentisierung,

sondern auch weitere persönliche Daten zur Verfügung gestellt werden, wenn es darum geht, die aufgebaute Verbindung für bestimmte Zwekke, beispielsweise Online-Banking oder dergleichen, zu verwenden.

[0011] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß die Identifizierungs- beziehungsweise Authentisierungsdaten unter einem Hauptschlüssel und entsprechend einer Schlüsselhierarchie darunter angeordneten, spezifischen Schlüsseln abgelegt werden. Damit ergibt sich in vorteilhafter Weise eine Möglichkeit, einzelnen Bereiche des Kommunikationsmoduls für den Zugang individuell abzusichern und damit eine erhöhte Sicherheit bei der Verwendung des Kommunikationsmoduls zu erreichen.

[0012] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß der Hauptschlüssel bereits beim Herstellen des Kommunikationsmoduls eingespeichert wird, wodurch sichergestellt wird, daß der Kommunikationsmodul nicht bereits bei der ersten Inbetriebnahme manipuliert wird.

[0013] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß die spezifischen Schlüssel nach einem cryptographischen Verfahren abgelegt werden, um die Sicherheit der Schlüssel zu erhöhen.

[0014] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß relevante Daten und Programme, insbesondere die Daten für den Kommunikationsaufbau und die persönlichen Daten sowie die Programme und Steuerungsparameter, in dem Kommunikationsmodul in einem geschützten Speicherbereich nicht-manipulierbar gespeichert werden, so daß in vorteilhafter Weise ein Mißbrauch des Kommunikationsmoduls erheblich erschwert wird.

[0015] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß in dem Kommunikationsmodul Programme gespeichert werden, die bei Aktivierung durch den Anwender oder einen Kommunikationspartner im Netz entsprechend an sich bekannter Protokolle und an sich bekannter Identifizierungs- oder Authentisierungs-Prozeduren sowie durch die persönlichen Daten und zum Verbindungsaufbau erforderlichen Parameter gesteuert durch das Anwendergerät über eine Geräteschnittstelle von dem Kommunikationsmodul in den Nachrichtenstrom eingeblendet werden. Somit kann der Kommunikationsmodul sowohl von sich aus eine Verbindung mit dem gewünschten Netz herstellen, während er auch selbst über das Netz aktiviert werden kann, so daß eine Verbindung von einem Netzteilnehmer über den Kommunikationsmodul zu dem Anwendergerät hergestellt wird.

[0016] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß zur Identifizierung oder Authentisierung des Anwenders gegenüber dem Kommunikationsmodul eine PIN und/oder ein Paßwort in dem Kommunikationsmodul gespeichert werden und daß die PIN oder das Paßwort vom Anwender über das Anwendergerät eingegeben wird. Dadurch kann einerseits sichergestellt werden, da0 nur ein berechtigter Anwender den Kommunikationsmodul durch Eingabe einer PIN funktionsbereit machen kann, andererseits kann der Anwender jederzeit eine Änderung der PIN vornehmen, um beispielsweise beim Ausspähen der PIN durch einen Unberechtigten Mißbrauch vorbeugen. Des Weiteren können in vorteilhafter Weise der Aufwand für den Kommunikationsmodul gesenkt und damit die Kosten reduziert werden, da das Anwendergerät als Eingabegerät für den Kommunikationsmodul benutzt wird.

[0017] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß zur Identifizierung oder Authentisierung des Anwenders ein biometrisches Referenzmuster, vorzugsweise ein Sprachmuster oder ein Fingerabdruck, in dem Kommunikationsmodul gespeichert wird, und daß das biometrische Muster von dem Anwender über einen Sensor in den Kommunikationsmodul verifiziert wird. Durch den zusätzlichen Sensor, der das biometrische Muster des Anwenders erfassen kann, wird eine Möglichkeit geschaffen, eine berechtigte Nutzung des Kommunikationsmoduls und den Zugriff auf den Kommunikationsmodul außerordentlich sicher zu gestalten.

[0018] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß die Daten oder Informationen durch einen Crypto-Controller in dem Kommunikationsmodul verschlüsselt beziehungsweise entschlüsselt werden, so daß eine erhöhte Sicherheit dadurch gegeben ist, daß in dem gekapselten Kommunikationsmodul cryptographische Verfahren unter Verwendung der im Kommunikatonsmodul gespeicherten Schlüssel angewendet werden.

[0019] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß eine Information an einem Anzeigefeld an dem Kommunikationsmodul angezeigt wird. Damit ergibt sich in vorteilhafter Weise eine Möglichkeit, die Information zu überprüfen und gegebenenfalls neu einzugeben, falls sie geändert werden sollen oder eine Manipulation der Information festgestellt wurde, bevor eine Transaktion ausgelöst wird.

[0020] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß der Netzanschluß im Kommunikationsmodul durch eine zusätzliche netzseitige Schnittstelle von der Steuerung des Kommunikationsmoduls entkoppelt ist. Damit kann der Kommunikationsmodul in vorteilhafter Weise mit Unterschiedlichen Netzanschlüssen ausgestattet werden und bei Ausstattung mit mehreren Anschlüssen könne die Verbindungen in vorteilhafter Weise, zum Beispiel mit einem Mobilnetz und einem Festnetz, durch einfaches Auswählen des zutreffenden Anschlusses bewerkstelligt werden.

[0021] Eine weitere vorteilhafte Ausführungsform der Erfindung ist dadurch gekennzeichnet, daß in dem Kommunikationsmodul bei der Einleitung eines aus

ı Netz angestoßenen Verbindungsaufbaus feststellt, ın das Gerät, in das der Kommunikationsmodul einteckt ist, für die angeforderte Kommunikation nicht ignet ist. Damit kann in vorteilhafter Weise dem ımunikationspartner in Netz und an Gerät eine kmeldung gegeben werden. Des Weiteren kann der ımunikationsmodul diesen Vorgang speichern, um h dem Einstecken des Kommunikationsmoduls in geeignetes Gerät eine Nachricht an das Gerät abzu-en.

[22] Die Einrichtung zum Aufbauen einer Kommikation zwischen einem Anwendergerät und einem z ist erfindungsgemäß gekennzeichnet durch einen sönlichen Kommunikationsmodul, in dem persönliDaten sowie Informationen über den Kommunikatiaufbau zwischen unterschiedlichen Anwenderäten und Netzen bereitgestellt sind.

[23] Mit dieser Einrichtung und deren vorteilhafAusgestaltungen, die in den restlichen Unteransprün gekennzeichnet sind, lassen sich die sprechenden Vorteile erreichen, wie sie oben im ammenhang mit den Verfahrensansprüchen angeen sind.

[24] Ausführungsbeispiele der Erfindung werden anhand der beiliegenden Zeichnungen beschrie-. Es zeigen:

Figur 1 eine schematische Darstellung der Struktur des persönlichen Kommunikationsmoduls gemäß einem Ausführungsbeispiel der Erfindung;

Figur 2 eine Schlüsselhierarchie, wie sie in dem Kommunikationsmodul verwirklicht sein kann;

Figur 3 eine abgewandelte Ausführungsform des persönlichen Kommunikationsmoduls in schematischer Darstellung; und

Figur 4 eine perspektivische Darstellung des Kommunikationsmoduls als Gerät.

[25] In Figur 1 ist ein persönlicher Kommunikatimodul nach einem Ausführungsbeispiel der ıdung schematisch dargestellt. Der Kommunikatimodul 2 umfaßt eine Geräteschnittstelle 4 zum rendergerät, ein Rechner 6, einen Arbeitsspeicher inen Speicher 10 für ein Betriebssystem, einen icher 12 für die Programme und die Daten, sowie n Netzschnittstellenmodul 14. Die Elemente des ımunikationsmoduls sind über einen Bus 16 miteiner verbunden. Mit der Gerateschnittstelle 4 wird der ımunikationsmodul 2 an ein Anwendergerät eckt, während der Netzschnittstellenmodul 14 zum chluß an ein Netz vorgesehen ist.

[26] Der Speicher 12 für die Programme und die n kann nach heutigem Stand der Technik ein ROM-Speicher oder ein sogenannter Flash-Speisein. Jedenfalls muß der Speicher geeignet sein, anwenderspezifische Daten auch im spannungslosen Zustand zu speichern und auch Änderungen dieser Daten zuzulassen.

[0027] Figur 2 zeigt eine Schlüsselhierarchie, wie sie in dem Kommunikationsmodul, insbesondere in dem EEPROM-Speicher 12 verwirklicht sein kann. Es ist ein Hauptschlüssel vorgesehen, der den Erstzugriff zu dem Kommunikationsmodul kontrolliert. Für den Zugriff auf Speicherbereiche des Kommunikationsmoduls und zur Sicherung von Kommunikationsvorgängen sind in der Schlüsselhierarchie mehrere Unterschlüssel vorgesehen, die beispielsweise verschiedenen Serviceprovidern 1...n, Service-Leistungen 1...n im Bereich der einzelnen Serviceprovider sowie Resourcen 1...n des Anwenders absichern.

[0028] Figur 3 ist eine abgewandelte Ausführungsform des persönlichen Kommunikationsmoduls 20 in schematischer Darstellung. Wie der Kommunikationsmodul 2 weist auch der Kommunikationsmodul 20 eine Geräteschnittstelle 24, einen Rechner 26 (CPU), einen Arbeitsspeicher 28 (RAM), einen Betriebssystemspeicher 30 (ROM), einen Speicher 32 für die Programme und die Daten sowie einen Netzschnittstellenmodul 34 auf. Die Elemente des Kommunikationsmoduls 20 sind über einen Bus 36 miteinander verbunden. Zusätzlich weist der Kommunikationsmodul 20 einen Sensor 38 auf, der zur Identifizierung oder Authentisierung des Anwenders durch ein biologisches Muster, vorzugsweise ein Sprachmuster oder einen Fingerabdruck, dient. Das biometrische Muster ist in dem Speicher 32 gespeichert, und, wenn ein Zugriff auf den Kommunikationsmodul 20 erwünscht ist, wird das biometrische Muster des Anwenders über den Sensor 38 am Kommunikationsmodul 20 eingegeben. In dem Kommunikationsmodul 20 wird dann die Übereinstimmung der beiden biometrischen Muster überprüft, und bei positivem Ergebnis wird der Zugang zu dem Kommunikationsmodul 20 ermöglicht.

[0029] Der Kommunikationsmodul 20 gemäß Figur 3 umfaßt weiterhin einen Crypto-Controller 40, der dazu dient, die Daten oder Informationen in dem Kommunikationsmodul 20 zu verschlüsseln beziehungsweise zu entschlüsseln, um die Sicherheit des Kommunikationsmoduls zu verbessern.

[0030] Des Weiteren ist bei dem Ausführungsbeispiel von Figur 3 ein Anzeigenfeld 42 vorgesehen, an dem Informationen der Anwender überprüfen möchte oder bestätigen soll angezeigt werden können.

[0031] Schließlich weist die Ausführungsform von Figur 3 noch einen zusätzlichen Netzschnittstellenmodul 44 auf, der unterschiedliche Netzanschlüsse umfaßt, so daß auf einfache Weise eine Verbindung mit einem Festnetz 46 oder einem Mobilnetz 48 aufgebaut werden kann, in dem lediglich die geeigneten Abschlüsse an dem Netzschnittstellenmodul 44 ausgebildet werden.

[0032] Figur 4 zeigt eine schematische, perspektivische Darstellung des Kommunikationsmoduls als

Gerät. Es kann sich dabei um den Kommunikationsmodul 2 oder den Kommunikationsmodul 20 handeln. Der Kommunikationsmodul hat ein Gehäuse 50 und einen Steckanschluß 52, mit dem er in eine entsprechende Schnittstellenbuchse an dem Anwendergerät eingesteckt werden kann. Da eine weitgehende Normung von Schnittstellen heutzutage üblich ist, kann ein derartiger Kommunikationsmodul mit einer großen Vielzahl von Anwendergeräten verwendet werden.

[0033] Im folgenden wird der Ablauf bei dem Verbindungsaufbau beziehungsweise die Betriebsweise des Kommunikationsmoduls beschrieben. Die Personalisierung, das heißt das Laden des Kommunikationsmoduls mit Identifikations-, Authentisierungsparametern, persönlichen Daten und Programmen erfolgt nach einem an sich bekannten Verfahren, wie es bei Prozessorchipkarten üblich ist. Aus dem eindeutigen Hauptschlüssel können von Serviceprovidern oder Dienstanbietern oder vom Anwender selbst weitere spezifische Schlüssel entsprechend einer Schlüsselhierarchie generiert werden, und der Hauptschlüssel sowie die speziellen Unterschlüssel können in dem Kommunikationsmodul nicht manipulierbar abgespeichert werden. Mittels dieser Schlüssel können dann Parameter und Daten im geschützten Speicherbereich des Kommunikationsmoduls sowie Kommunikationsvorgänge und Netzrecoursen gesichert werden.

[0034] Wird eine Kommunikation durch den Anwender eingeleitet, erhält der im Anwendergerät gesteckte Kommunikationsmodul über die Geräteschrittstelle einen entsprechenden Code, der den Kommunikationsmodul veranlaßt, den Verbindungsaufbau zum persönlichen Kommunikationspartner zu starten. Während des Verbindungsaufbaus werden, entsprechend bekannter Protokolle und Anwendungsverfahren, die Identifikations- und Authentisierungsparameter, beispielsweise Paßwort, Benutzer-ID, private Schlüssel, Zertifikat des öffentlichen Schlüssels, gesteuert durch das Anwendergerät, über die Geräteschnittstelle vom Kommunikationsmodul in den Nachrichtenstrom eingeblendet. Nach positivem Verbindungsaufbau können, gesteuert durch das Anwendergerät, auch persönliche Daten oder beispielsweise Autorisierungsparameter von dem Kommunikationsmodul in den Nachrichtenstrom eingeblendet werden. Im Anwendergerät und im Kommunikationsmodul können Abläufe programmiert sein, um die zum Verbindungsaufbau erforderlichen Parameter, beispielsweise Telefonnummern, IP-Adressen, Mailadressen und dergleichen, aus einem Speicherbereich des Kommunikationsmoduls zu selektieren und entsprechend den Kommunikationsprotokollen einzublenden.

[0035] Wird eine Kommunikation durch einen Kommunikationspartner im Netz eingeleitet, erkennt der gesteckte Kommunikationsmodul das eingehende Signal und aktiviert das Anwendergerät, um einen Verbindungsaufbau herzustellen. Erforderliche Authentisierungsparameter während des Verbindungsaufbaus, beziehungsweise Autorisierungsparameter im Verfahren, werden von dem Kommunikationsmodul, gesteuert durch das Anwendergerät, eingeblendet wie oben beschrieben wurde.

[0036] Eine persönliche Identifikation des Anwenders durch den Kommunikationsmodul kann wie folgt durchgeführt werden. Nach Einstecken des Kommunikationsmoduls in ein Anwendergerät startet der Anwender am Gerät eine Identifikationsprozedur. Dabei gibt er an der Tastatur des Anwendergerätes eine PIN (persönliche Identifikationsnummer) ein. Das Anwendergerät übergibt über die Geräteschnittstelle die PIN mit einem Identifikationscode an den Kommunikationsmodul. Der Kommunikationsmodul vergleicht die PIN mit einer bei der Personalisierung des Kommunikationsmoduls eingespeicherten Referenzzahl. Bei einem positiven Ergebnis schaltet der Kommunikationsmodul seine Grundfunktionen frei. Statt mit einer PIN kann die Identifikation auch mit Paßwörtern oder biometrischen Mustern durchgeführt werden, wie oben beschrieben wurde. In dem Kommunikationsmodul können bei der Personalisierung entsprechende Paßwörter oder Referenzmuster gespeichert werden.

[0037] Der bereits erwähnte Sensor dient zur Erhöhung der Sicherheit bei der persönlichen Identifikation des Anwenders bei dem Kommunikationsmodul. Nach Einstecken des Kommunikationsmoduls in das Anwendergerät schaltet der Kommunikationsmodul seine Grundfunktionen erst nach positiver Verifikation des am Sensor erkannten biometrischen Musters frei. Der Crypto-Controller ist für asymmetrische Verschlüsselungsverfahren ausgelegt und erhöht in dem Kommunikationsmodul die Sicherheit bei den Authentisierungs- und Autorisierungsverfahren. Der Kommunikationsmodul führt die Verschlüsselung/Entschlüsselung eigenständig durch und erzeugt digitale Signaturen. Damit sind Manipulationsmöglichkeiten von außen praktisch nicht mehr gegeben. Gleichzeitig kann die Sicherheit beim Laden von sensiblen Schlüsseln oder Daten einerseits von der Anwendergeräteseite und andererseits über den Netzanschluß erheblich gesteigert werden.

[0038] Der Kommunikationsmodul kann beispielsweise auch an Automaten eingesteckt werden, um beispielsweise nach Auswahl einer Ware oder eines Tickets einen Zahlvorgang über ein Netz abzuwikkeln. In diesem Fall ist aus Sicherheitsgründen ein Anzeigenfeld im Kommunikationsmodul vorgesehen. In diesem Feld wird unter Steuerung des Automaten der Zahlbetrag für das ausgewählte Objekt angezeigt, so daß der Benutzer sich von der Richtigkeit seiner Angaben überzeugen kann, bevor er eine On-line-Transaktion auslöst.

[0039] Zum Bezahlen von kleineren Beträgen eignet sich besonders eine elektronische Geldbörse, wie sie beispielsweise bereits in der deutschen Geldkarte verwirklicht ist. Der Kommunikationsmodul mit seinen Sicherheitsmerkmalen kann nach den bekannten Konventionen eine oder mehrere elektronische Geldbörsen beinhalten. Das Auf- oder Abbuchen von Geldbeträgen kann von Anwendergeräten nach bekannten Verfahren

wickelt werden. Der Kommunikationsmodul verhält dabei wie ein Chipkartenleser mit eingesteckter karte mit der Anwendung „elektronische Geld-e". Bei der Ausführungsform von Figur 3 mit dem tzlichen Netzschnittstellenmodul 44 werden die anschlüsse für das Festnetz 46 und das Mobilnetz on dem eigentlichen Kommunikationsmodul entelt. Damit lassen sich mit demselben Kommunikamodul unterschiedliche Netzanschlüsse, ielsweise GSM, DECT, UMTS, IR, ISDN, DVB-C, ieren oder beispielsweise mehrere Mobilfunknetze hiedener Frequenzen, beispielsweise GSM 800 1900 oder auch ein Mobilnetzanschluß und ein ietzanschluß, beispielsweise GSM und ISDN, parealisieren.

ntansprüche

Verfahren zum Aufbauen einer Kommunikation zwichen einem Anwendergerät und einem Netz, **adurch gekennzeichnet, daß** persönliche Daten owie Informationen über den Kommunikationsaufau zwischen dem Anwendergerät und dem Netz in inem in unterschiedlichen Geräte steckbaren, perönlichen Kommunikationsmodul gespeichert werlen und daß die Daten und die Informationen zum ufbau der Kommunikation abgerufen werden.

Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** der persönliche Kommunikationsodul mit den Identifikations- und Authentiierungsdaten sowie persönlichen Daten seines esitzers beziehungsweise Anwenders mechaisch gekapselt werden.

Verfahren nach Anspruch 1 oder 2, **dadurch ekennzeichnet, daß** auch die Programme zum ommunikationsaufbau in dem Kommunikationsodul gespeichert werden.

Verfahren nach einem der Ansprüche 1 bis 3, **adurch gekennzeichnet, daß** die persönlichen aten solche zum Identifizieren oder Authentisieen sowie personenbezogene Daten umfassen.

Verfahren nach Anspruch 4, **dadurch gekennzeichnet, daß** die Identifizierungs- beziehungseise Authentisierungsdaten unter einem auptschlüssel und entsprechend einer Schlüsselierarchie darunter angeordneten, spezifischen chlüsseln abgelegt werden.

Verfahren nach Anspruch 5, **dadurch gekennzeichnet, daß** der Hauptschlüssel bereits beim erstellen des Kommunikationsmoduls eingespeihert wird, wodurch sichergestellt wird, daß der ommunikationsmodul nicht bereits bei der ersten betriebnahme manipuliert wird.

7. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, daß** die spezifischen Schlüssel nach einem cryptographischen Verfahren abgelegt werden, um die Sicherheit der Schlüssel zu erhöhen.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, daß** daß relevante Daten und Programme, insbesondere die Daten für den Kommunikationsaufbau und die persönlichen Daten sowie die Programme und Steuerungsparameter, in dem Kommunikationsmodul in einem geschützten Speicherbereich nicht-manipulierbar gespeichert werden.

9. Verfahren nach Anspruch 3, **dadurch gekennzeichnet, daß** in dem Kommunikationsmodul Programme gespeichert werden, die bei Aktivierung durch den Anwender oder einen Kommunikationspartner im Netz, entsprechend an sich bekannter Protokolle und an sich bekannter Identifizierungs- oder Authentisierungs-Prozeduren sowie durch die persönlichen Daten und zum Verbindungsaufbau erforderlichen Parameter, gesteuert durch das Anwendergerät über eine Geräteschnittstelle, von dem Kommunikationsmodul in den Nachrichtenstrom eingeblendet werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, daß** zur Identifizierung oder Authentisierung des Anwenders gegenüber dem Kommunikationsmodul eine PIN und/oder ein Paßwort in dem Kommunikationsmodul gespeichert werden und daß die PIN oder das Paßwort vom Anwender über das Anwendergerät eingegeben wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, daß** zur Identifizierung oder Authentisierung des Anwenders ein biometrisches Referenzmuster, vorzugsweise ein Sprachmuster oder ein Fingerabdruck, in dem Kommunikationsmodul gespeichert wird, und daß das biometrische Muster von dem Anwender über einen Sensor in den Kommunikationsmodul verifiziert wird.

12. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, daß** die Daten oder Informationen durch einen Crypto-Controller in dem Kommunikationsmodul verschlüsselt beziehungsweise entschlüsselt werden.

13. Verfahren nach einem der vorhergehenden Ansprüche, **dadudch gekennzeichnet, daß** eine Information an einem Anzeigefeld an dem Kommunikationsmodul angezeigt wird.

14. Verfahren nach einem der vorhergehenden Ansprü-

che, **dadurch gekennzeichnet, daß** der Netzanschluß im Kommunikationsmodul durch eine zusätzliche netzseitige Schnittstelle von der Steuerung des Kommunikationsmoduls entkoppelt ist.

15. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, daß** in dem Kommunikationsmodul bei der Einleitung eines aus dem Netz angestoßenen Verbindungsaufbaus feststellt, wenn das Gerät, in das der Kommunikationsmodul eingesteckt ist, für die angeforderte Kommunikation nicht geeignet ist.

16. Einrichtung zum Aufbauen einer Kommunikation zwischen einem Anwendergerät und einem Netz, **gekennzeichnet durch** einen persönlichen Kommunikationsmodul, in dem persönliche Daten sowie Informationen über den Kommunikationsaufbau zwischen unterschiedlichen Anwendergeräten und Netzen bereitgestellt sind.

17. Einrichtung nach Anspruch 16, **dadurch gekennzeichnet, daß** der persönliche Kommunikationsmodul mit den Identifikations- und Authentisierungsdaten sowie persönlichen Daten seines Besitzers beziehungsweise Anwenders mechanisch gekapselt sind.

18. Einrichtung nach Anspruch 17, **dadurch gekennzeichnet, daß** sie über eine Standardschnittstelle mit dem Anwendergerät zu verbinden ist.

19. Einrichtung nach Anspruch 16, **dadurch gekennzeichnet, daß** auch die Programme zum Kommunikationsaufbau in dem Kommunikationsmodul bereitgestellt sind.

20. Einrichtung nach Anspruch 16, **dadurch gekennzeichnet, daß** der Kommunikationsmodul eine Schnittstelle (4, 24) zum Anwendergerät eine Recheneinheit (6, 26), einen Arbeitsspeicher (8, 28), einen Speicher (10, 30) für ein Betriebssystem (12, 32) für die Programme und die Daten sowie einen Netzschnittstellenmodul (14, 34) aufweist.

21. Einrichtung nach Anspruch 16, **dadurch gekennzeichnet, daß** die persönlichen Daten solche zum Identifizieren oder Authentisieren sowie personenbezogene Daten umfassen.

22. Einrichtung nach Anspruch 21, **dadurch gekennzeichnet, daß** die Identifizierungs- beziehungsweise Authentisierungs-Daten unter einem Hauptschlüssel und entsprechend einer Schlüsselhierarchie darunter angeordneten, spezifischen Schlüsseln abgelegt sind.

23. Verfahren nach Anspruch 22, **dadurch gekennzeichnet, daß** der Hauptschlüssel bereits beim Herstellen des Kommunikationsmoduls eingespeichert wird, wodurch sichergestellt wird, daß der Kommunikationsmodul nicht bereits bei der ersten Inbetriebnahme manipuliert wird.

24. Verfahren nach Anspruch 22, **dadurch gekennzeichnet, daß** die spezifischen Schlüssel nach einem cryptographischen Verfahren abgelegt werden, um die Sicherheit der Schlüssel zu erhöhen.

25. Einrichtung nach einem der Ansprüche 16 bis 24, **dadurch gekennzeichnet, daß** die persönlichen Daten in dem Kommunikationsmodul in einem geschützten Speicherbereich nicht-manipulierbar gespeichert sind.

26. Einrichtung nach einem der Ansprüche 16 bis 25, **dadurch gekennzeichnet, daß** der Kommunikationsmodul Programme umfaßt, die bei Aktivierung durch den Anwender oder einen Kommunikationspartner im Netz entsprechend an sich bekannter Protokolle und an sich bekannter Identifizierungs- oder Authentisierungs-Prozeduren sowie die persönlichen Daten und zum Verbindungsaufbau erforderlichen Parameter, gesteuert durch das Anwendergerät, über eine Geräteschrittstelle von dem Kommunikationsmodul in den Nachrichtenstrom einblenden.

27. Einrichtung nach einem der Ansprüche 16 bis 26, **dadurch gekennzeichnet, daß** zur Identifizierung oder Authentisierung des Anwenders eine PIN und/oder ein Paßwort in dem Kommunikationsmodul gespeichert ist, und daß die PIN oder das Paßwort vom Anwender über das Anwendergerät einzugeben ist.

28. Einrichtung nach einem der Ansprüche 16 bis 27, **dadurch gekennzeichnet, daß** zur Identifizierung oder Authentisierung des Anwenders ein biometrisches Muster, vorzugsweise ein Sprachmuster oder ein Fingerabdruck, in dem Kommunikationsmodul gespeichert ist und daß das biometrische Muster über einen Sensor (38) am Kommunikationsmodul eingegeben ist.

29. Einrichtung nach einem der Ansprüche 16 bis 28, **gekennzeichnet durch** einen Crypto-Controller (40) in dem Kommunikationsmodul.

30. Einrichtung nach einem der Ansprüche 16 bis 29, **gekennzeichnet durch** ein Anzeigenfeld (42) an dem Kommunikationsmodul.

31. Einrichtung nach einem der Ansprüche 16 bis 30, **gekennzeichnet durch** eine zusätzliche, netzseitige Schnittstelle (44), die unterschiedliche Netzan-

schlüsse umfaßt.

Einrichtung nach einem der Ansprüche 16 bis 31, **dadurch gekennzeichnet, daß** indem Kommunikationsmodul bei der Einleitung eines aus dem Netz angestoßenen Verbindungsaufbaus feststellt, wenn das Gerät, in das der Kommunikationsmodul eingesteckt ist, für die angeforderte Kommunikation nicht geeignet ist.

FIG 1

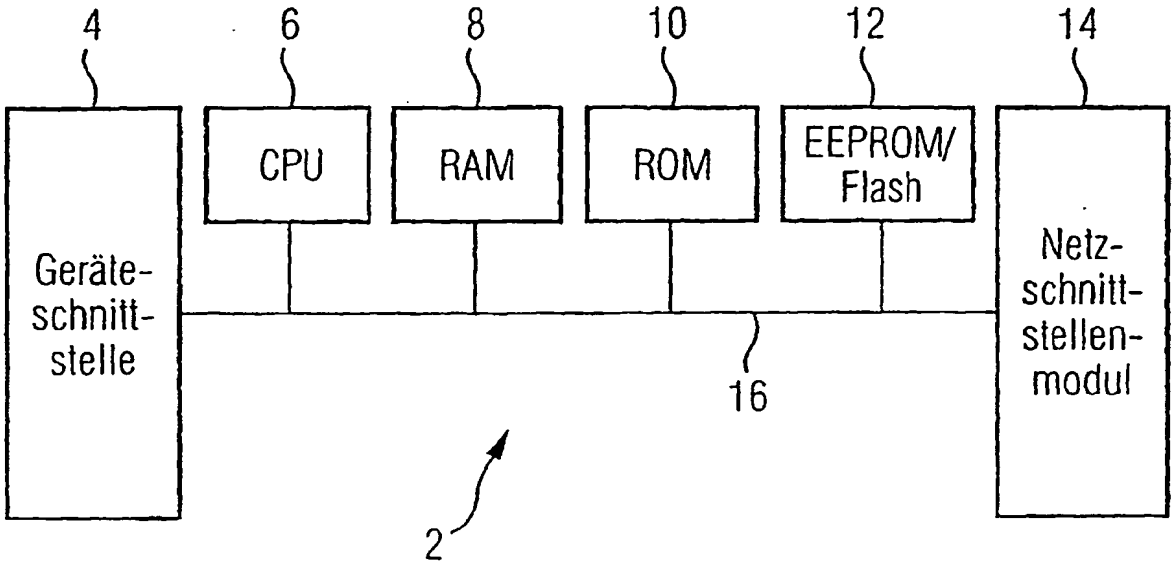

4
6
8
10
12
14
Geräte-schnitt-stelle
CPU
RAM
ROM
EEPROM/ Flash
Netz-schnitt-stellen-modul
16
2

FIG 2

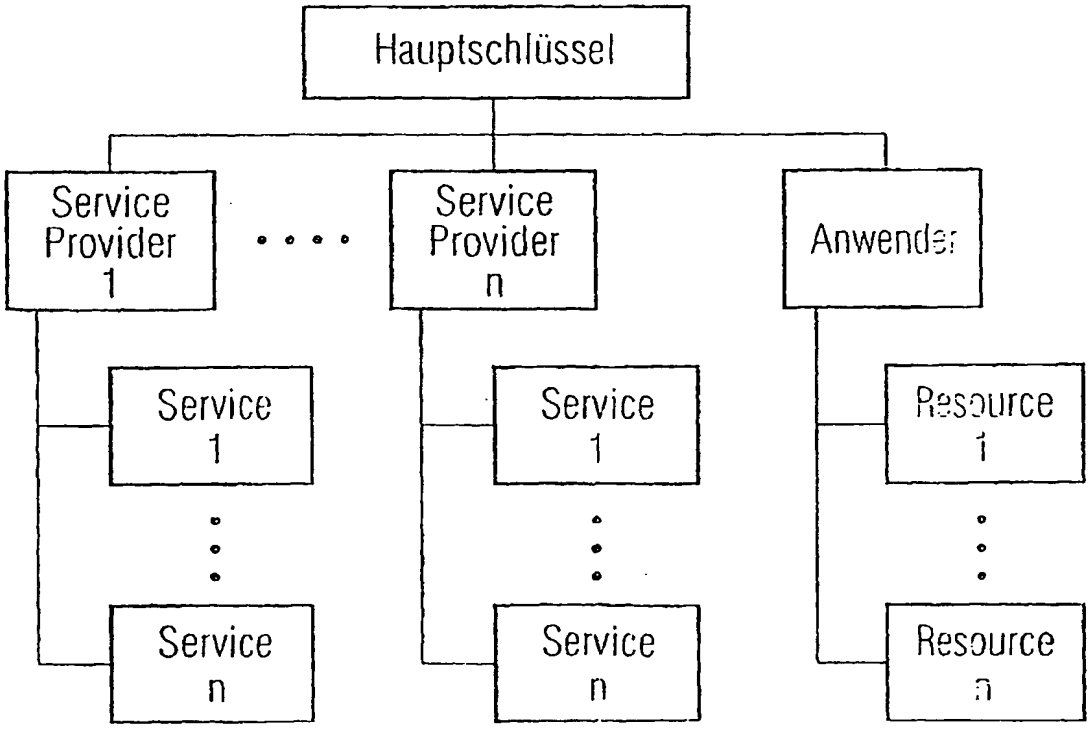

Hauptschlüssel
Service Provider 1
Service Provider n
Anwender
Service 1
Service n
Service 1
Service n
Resource 1
Resource n

FIG 3

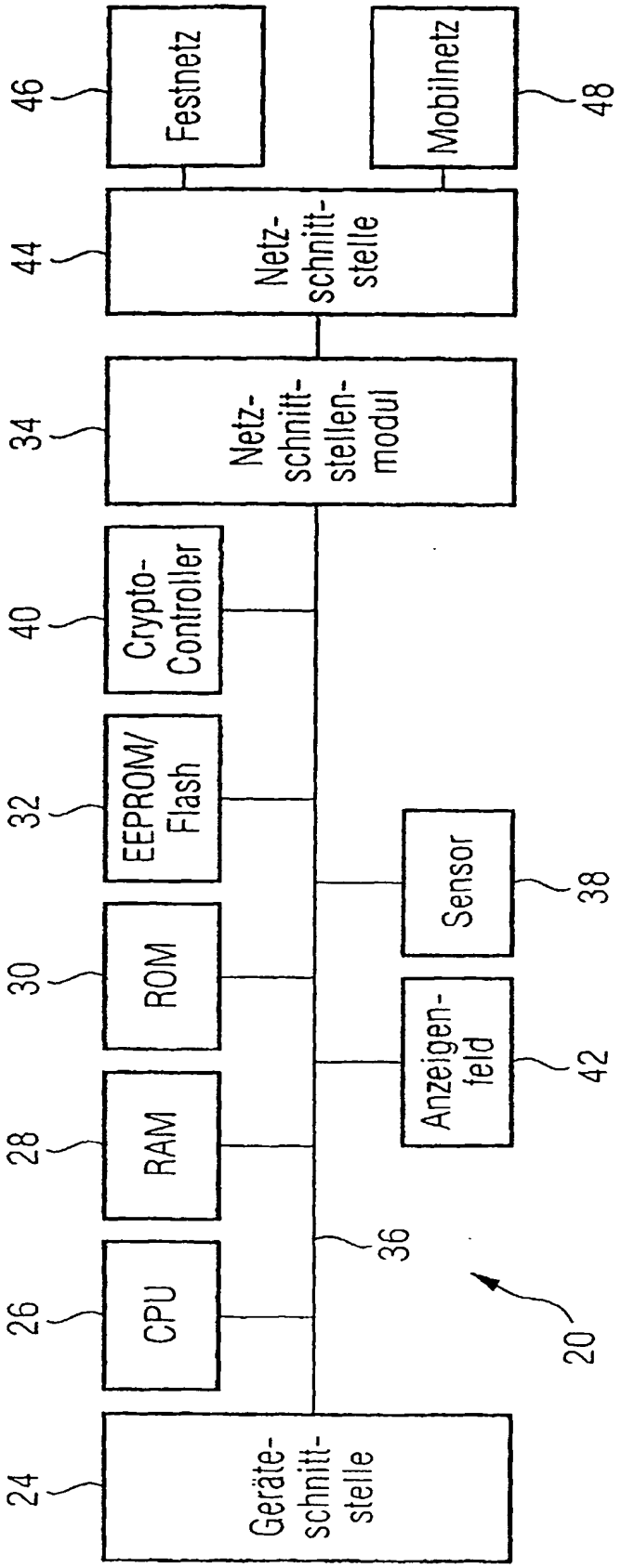
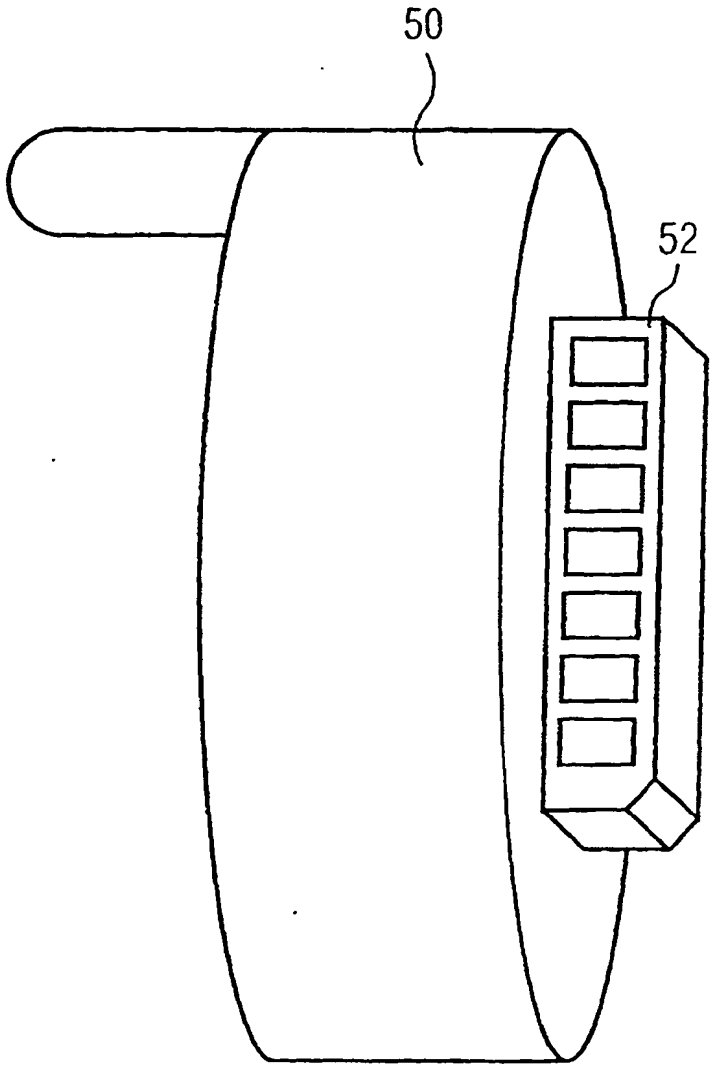

Festnetz
46
Mobilnetz
48
Netz-schnitt-stelle
44
Netz-schnitt-stellen-modul
34
Crypto-Controller
40
EEPROM/ Flash
32
ROM
30
RAM
28
CPU
26
Sensor
38
Anzeigen-feld
42
36
20
Geräte-schnitt-stelle
24

FIG 4



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 063 862 A3

(12) EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:
03.01.2001 Patentblatt 2001/01

(43) Veröffentlichungstag A2:
27.12.2000 Patentblatt 2000/52

(21) Anmeldenummer: **00112588.9**

(22) Anmeldetag: **14.06.2000**

(51) Int. Cl.[7]: **H04Q 7/38**, H04Q 7/32

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **25.06.1999 DE 19929251**

(71) Anmelder:
Fujitsu Siemens Computers GmbH
81739 München (DE)

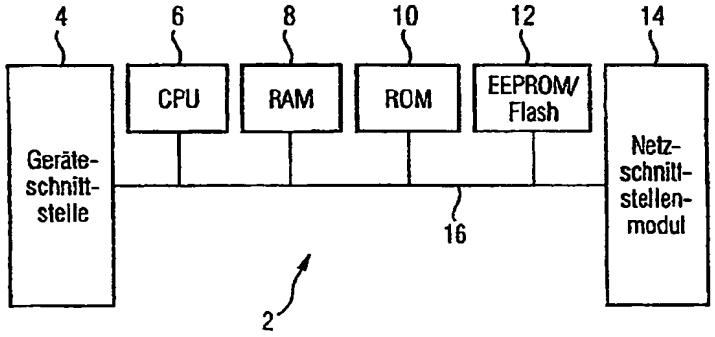
(72) Erfinder: **Wiehler, Gerhard**
82223 Eichenau (DE)

(74) Vertreter:
Epping, Wilhelm, Dipl.-Ing. et al
Epping Hermann & Fischer
Postfach 12 10 26
80034 München (DE)

(54) Verfahren und Einrichtung zum Aufbau einer Kommunikation zwischen einem Anwendergerät und einem Netz

(57) Es wird ein Verfahren und eine Einrichtung zum Aufbauen einer Kommunikation zwischen einem Anwendergerät und einem Netz angegeben, wobei persönliche Daten und Informationen sowie Programme über den Kommunikationsaufbau zwischen dem Anwendergerät und dem Netz in einem persönlichen Kommunikationsmodul gespeichert und die Daten und die Informationen zum Aufbau der Kommunikation abgerufen werden.

FIG 1



Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 00 11 2588

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	WO 98 58510 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 23. Dezember 1998 (1998-12-23) * Seite 5, Zeile 17 - Seite 8, Zeile 15 *	1,2,4, 8-10,14, 16-18, 20,21, 25-27,31	H04Q7/38 H04Q7/32
A	DE 40 12 931 A (SCHREIBER HANS) 31. Oktober 1991 (1991-10-31) * Spalte 1, Zeile 3 - Spalte 2, Zeile 51 *	1,2,4,8, 10, 16-18, 20,21, 25,27	
A	WO 98 44412 A (HOFMANN LUDWIG ;SIEMENS AG (DE)) 8. Oktober 1998 (1998-10-08) * Seite 4, Zeile 9 - Seite 5, Zeile 22 *	1-3, 16-19	
A	LAPERE ET AL: "User Authentication in Mobile Telecommunication Environments Using Voice Biometrics and Smartcards" PROCEEDINGS. INTERNATIONAL CONFERENCE ON INTELLIGENCE IN SERVICES AND NETWORKS, 27. Mai 1997 (1997-05-27), XP002106691 * Seite 437, Zeile 40 - Seite 439, Zeile 45 *	10,11, 27,28	

RECHERCHIERTE SACHGEBIETE (Int.Cl.7)
H04Q

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	13. November 2000	Weinmiller, J

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C09)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 00 11 2588

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

13-11-2000

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9858510 A	23-12-1998	WO 9858509 A	23-12-1998
		AU 3022497 A	04-01-1999
		AU 5649598 A	04-01-1999
		CN 1260939 T	19-07-2000
		EP 0990355 A	05-04-2000
		EP 0990356 A	05-04-2000
		NO 996145 A	16-02-2000
		NO 996148 A	11-02-2000
DE 4012931 A	31-10-1991	KEINE	
WO 9844412 A	08-10-1998	AU 6608498 A	22-10-1998
		CN 1246185 T	01-03-2000
		EP 0970422 A	12-01-2000

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82